Learning Lessons from Countering Terrorism: the UK Experience 2017–2020

Neil Basu¹

Accepted: 16 August 2021 / Published online: 16 September 2021
© The Author(s), under exclusive licence to Springer Nature Switzerland AG 2021

Abstract

Research Question What lessons can be learned from counter-terrorism policing in a recent 3-year time period in which the UK suffered the loss of 41 lives by 12 terrorist attacks, with the concurrent successful disruption of 29 other attacks?

Data A 2017 internal review into the 2017 attacks was undertaken by police and MI5, yielding 104 recommendations for improved practices. This list was later complemented by multiple reviews in 2018–2020 that led to more than 400 further recommendations for multiple counter terrorism partners.

Methods Thematic analysis of these 500+ recommendations led to the author's distillation, as a participant observer, of 8 key focal points for future efforts to prevent terrorist attacks.

Findings Eight themes uniting the recommendations for developing future CT practice emerged from the internal reviews, raising complex issues of (1) data, (2) partnerships, (3) right-wing terrorism, (4) the 625,000 crowded public spaces in the UK, (5) online harm, (6) management of convicted terrorists, (7) domestic growth of terrorism replacing overseas direction and (8) earlier onset of terrorist commitments, from age 13.

Conclusions These thematic findings led to four conclusions: (a) the Protect Duty will provide an improved framework for countering terrorism, (b) we must adapt to the changing nature of terrorists, (c) we must increase our efforts against online harm and (d) we must renew and sustain our commitment to the Prevent pillar of the CONTEST strategy, which is now and shall be fit for purpose.

Keywords Terrorism · The CONTEST strategy · Security services · Multi-agency partnerships · Artificial intelligence

✉ Neil Basu
Neil.Basu@college.pnn.police.uk

¹ Metropolitan Police Service and College of Policing, London, UK

Introduction

This paper is about learning lessons from experience to fight terrorist threats now and in the future. It is also about how to learn those lessons in complexity whilst remembering there is no value in those that can't be implemented because they are impossible, unlawful or impractical or lack political or public support.

The past 6 years have seen the fastest evolution and diversification of terrorist threats in living memory, from the emergence of ISIS and their sophisticated media strategy to exploit vulnerable targets, to the rise of right wing and single-issue terrorism, as well as increasing hostile state activity like the Salisbury poisonings.

As the UK National Lead for Counter Terrorism (CT) Policing, I have been at the centre of the UK CT machine since 2015, and I want to share some of the themes that may help future-proof that machine. They are global problems with no easy solutions.

The language of learning can be neutral so we must always remember that a CT lesson often means terrible tragedy. This paper is the result of police looking hard at ourselves when we were found wanting. The reality of spending a meaningful amount of time in terrorism is that people will die on your watch. It is for that reason we try to learn and develop our systems at the same time as fighting the good fight.

In 6 years, there have been over 500 recommendations from multiple reviews, not least the 'operational improvement review' of the five British 2017 attacks which CT Policing and MI5 conducted on ourselves, even as we coped with a huge volume of investigations and attack plots. I have described it as trying to fine-tune a Formula 1 car whilst it is still on the track setting lap records. Please don't underestimate the physical and emotional effort this entailed.

There are common themes. Cells of well-trained terrorists and sophisticated attack planning are still a problem, but it's no longer *the* problem. Now it's vulnerable, young minds and contagious ideas, thrown together in a permissive environment. You don't need to be a traditional terrorist to commit an act of terror. A twisted ideology, a cheap, blunt tool, and some people to murder is enough. It's that simple and it is the simplicity that makes CT complex. Online radicalisation has produced terrorism that is individual, dispersed, highly random and more ideologically agnostic. It is high volume risk that is an acute threat but becoming a chronic disease.

I will touch on the four pillars of the UK's CT strategy called CONTEST, and how they interact. These four pillars, or 4 Ps, are Pursue (finding and stopping terrorists), Protect (target hardening important sites and people), Prepare (so we can respond to and recover from an attack) and Prevent (stopping people becoming terrorists in the first place).

Methodology: a Participant-Observer

As the Metropolitan Police Service Assistant Commissioner for Specialist Operations (ACSO) since March 2018, I have led the CT effort in London and the UK policing response to the CONTEST strategy through co-ordinating the CT Policing network. This period has seen the rise of ISIS and Extreme Right-Wing Terrorism,

and the hostile state action of the Salisbury poisonings. The network works in lock step with MI5, who hold the lead for UK domestic security. This partnership has responded to 12 attacks in the last 4 years but has prevented 29 more in what has probably been the most demanding period in our CT history since the height of the ‘Troubles’ and the prolific threat of Irish republicanism.

In 2017, I was the Senior National Coordinator with a long job description that boils down to working with MI5 to stop terrorist attacks—but on my watch 36 people died. I think about the victims every day, and probably always will. I took this job to try and stop there being any more. But more came. In 2017, the then Director General of MI5, Andrew (now Lord Andrew) Parker, described the threat as the worst he had seen in 34 years.

2017 did see an overhaul of the CT system and laws. I recognise the success of hard learned lessons but it’s not enough. Four years on we are still in a very difficult place. The move to simple methods of attack with little or no training required, as well as the growth in encrypted communications, creates two major frustrations which, taken together, put the UK in a constantly high risk position. Islamist Terrorism dominates by volume, but there is a smaller but significant threat from Extreme Right-Wing Terrorism, which continues to grow.

A Chronology of Attacks and Disruptions

Eight years separated the 2005, 7/7 bombings from the murder of British Army soldier Lee Rigby in the streets of London in 2013. Then another 4 years until the Westminster Bridge attack in March 2017.

Since the five attacks of 2017, there have been two Islamist attacks in 2018 in London and Manchester, where no-one was killed; two attacks in 2019—one the New Zealand-inspired Right Wing attack in Surrey, and the other the Islamist attack in Fishmongers Hall, London, where two young people were murdered.

2020 saw three Islamist attacks. The first resulted in the subject, under surveillance, being shot to death by police, but not before he managed to wound and traumatise innocent members of the public in a busy suburban London shopping street in Streatham. The second involved attacks on Prison Officers in a high security prison. The third in 2020 was in the city of Reading, just to the west of London, where in seconds an Islamist murdered three men before being arrested. He will never be released, but his victim’s families have also been handed a whole life sentence.

Since 2017 we have disrupted 29 plots, ten of them Extreme Right Wing terrorism (XRWT), one INCEL (involuntary celibacy)-inspired and the remaining Islamist. High volumes continue, with over 850 live investigations, a 30% plus increase on 2017; about 3000 current subjects of interest who remain a national security threat; and many tens of thousands now closed, but who were once investigated. Like Westminster, Manchester, Fishmongers Hall and Streatham, some may yet return to attack.

The context of threat is changing fast, with the pandemic, millions of deaths and an uncertain financial future. In the USA, we saw an attempted insurrection at the heart of a global democracy in Washington DC.

These concerns hit us before we had fully taken stock of the attacks of 2017–2020. We had difficult messages from the Westminster, London Bridge and Fishmongers Hall inquests. The Manchester Public Inquiry is still part heard with difficult revelations being broadcast every day. The Streatham and Salisbury Inquests have yet to start.

As we look back to ensure lessons are learned, we must look forward to understand emerging threats. We need to secure ourselves online and in the real world, and to land the right balance between target-hardening and the securitisation of our society.

Data: Recommendations from Internal Reviews

Without waiting for the lengthy and necessary multiple external reviews of each of these attacks, we have continuously and rapidly made our own judgements in CT command of the key lessons to be learned which totalled 104 recommendations. A 2017 internal review into the 2017 attacks was undertaken by police and MI5, yielding 104 recommendations for improved practices. This list was later complemented by multiple reviews in 2018–2020 that led to more than 400 further recommendations for multiple counter terrorism partners.

These recommendations have eight clear themes and focal points:

- First, the way we *collect, analyse and use data and then* share it inside the national security machine and with outside partners who could hold the vital key. Every inquest picks up a failure to communicate between agencies at some point. These days, the clue to stopping a terrorist is as likely to be found in a doctor, teacher or social worker's report as it is in a national security database.
- So the second focal point has to be *partnership*—and mobilising not just national security partners, but the business community and the public in *a whole society response*—not least the need for people to be alert to the reconnaissance, planning, renting and purchasing of materiel by terrorists, who are sometimes the most unremarkable figures, but who were leaving clues to their intent that collectively we just didn't see.
- Third, the *scourge of XRWT (extreme right wing terrorism)*, which was not appreciated for the threat it was and not dealt with in the same way as Islamist Terrorism.
- Fourth, the *failure to adequately protect crowded spaces*, lots of them with multiple owners but few with a sense of shared responsibility.
- Fifth, the lack of responsibility by social media giants and the *online harm* that the volume and speed of radicalising material was and is causing.
- Sixth, the *lack of attention to the committed terrorist once convicted*, radicalising others from the prison cell and still committed to murder on release.
- Seventh, the recognition that this *threat is no longer mainly trained and directed from abroad* but mostly caused by inspiring local, mostly younger boys and men, through social media.

- Eighth, when I say *younger, it's the phenomenon of the teenage terrorist*—our youngest target so far is 13 years old. Often these are mixed up kids unable to choose between violent ideologies and with complex psychological needs. We have a major social problem brewing in our homes and on the web, and COVID lockdowns will have made it worse.

These eight themes help to distil the essence of what 12 attacks and 29 disruptions has taught me over 4 years. It runs across all four CT pillars and all sections of society and it's not exhaustive. Failures across these themes conflate to increase the risk of extremism, the key driver behind all terrorist action.

Four Conclusions

To address these themes, I will concentrate on four conclusions that seem most pressing to me: the *Protect Duty*, the *Changing Nature of the Terrorist*, *Online Harm* and the *Prevent Programme*.

The Protect Duty

The Government has finished its consultation on 'The Protect Duty', which seeks to improve protective security and organisational preparedness in key locations and in a proportionate way. Complex problems need sophisticated solutions, which is why CONTEST is a multi-faceted programme, and why we seek to deliver all its elements in partnership. The 2017 review emphasised that we couldn't do it alone. The responsibility for stopping terrorism cannot rest with the national security CT machine alone; it needs wider government, local government and authorities, territorial law enforcement, businesses, health, education, communities and active citizen support.

We learned that the softest terrorist target is a publicly accessible place. The UK has 625,000 of them, and most can't be protected by intrusive security measures. As we target-harden the obvious iconic venues, we push terrorists to look elsewhere for any crowd. Fishmongers Hall, Streatham High Road, a Stanwell car park and a Reading public garden were *simple* attacks in *public* places with *no security*.

To counter such threat, we need partnerships with local authorities, businesses and major events organisers so they have to put in place appropriate CT measures. To provide such security consistently and at scale, we need a legal framework placing *more* responsibility on owners and administrators of potential targets.

It's right to require those responsible owners to keep the public safe, but it needs to be a proportionate and collaborative effort, not a legal sledgehammer. Change at this scale can only be done by having a shared ambition and that is to prevent there being more victims and survivors of terrorism.

Good security doesn't have to mean costly physical security. For many, it is staff training using products we have made freely available online. The security community will make sure that taking up CT guidance is cheap, easy and intuitive. We've

worked hard to provide online tools that can be used at scale. Our strapline—‘Action Counters Terrorism’ (ACT)—has been deployed to brand a suite of free online tools, and in as little as 45 min, staff can have the knowledge and confidence to spot and report suspicious behaviour, to understand what to do if attacked and how to make a plan. These simple measures could be the difference between life and death. We have over 10,000 organisations registered for this and over 600,000 learners have completed 2 million modules of training and its growing.

Changing Nature of the Terrorist

My second point is the changing nature of the terrorist. Their methodology has changed and so has the terrorist typology: they are no longer who we were fighting post 9/11. The rise of the ‘lone actor terrorist’ should now be our first concern but it’s an inaccurate description and was recently changed to ‘self-initiated’. They may carry out the final act alone but they seldom arise from a vacuum. They have usually spoken to someone in advance, or telegraphed their intentions, and often are the violent end product of an on or off-line radicaliser. ‘Lone actor’ implied they were impossible to predict, see or stop and never used propaganda or told others about their plans. That’s untrue. They *are* hard to see and stop but *not* impossible.

The dispersal of Daesh has reduced but not eradicated their online influence and their tactics have been copied by actors on the extreme right, who are also skilled online.

We are beginning to understand the difference between the self-initiated terrorist and terrorist cells. Their ideological position and consistency is different with the former much more volatile, shallow and unpredictable. They are less likely to be seen by us and more likely to be known to close contacts who may not recognise the danger until it’s too late.

At the heart of this shallow, ideological mixed-up terrorist is often an individual with complex needs and a range of vulnerabilities, and like a patient suffering from co-morbidities, improved outcomes require complex, clinical management. There is no single intervention that works for all of them.

Lengthy prison sentences have their place, but we know how extremism can flourish in prisons. Mental health treatment can play a part but we can be too dependent on its efficacy for a person living in chaos. Addictions, poverty, poor health, education, employment and structure all combine to drive feelings of isolation, exclusion, anger and potentially violence. People in these circumstances are easy prey for radicalisers.

The Protect Duty is the responsibility to protect vulnerable public spaces. We should apply that same effort to protect vulnerable minds. That needs a co-morbidity approach to vulnerable people, spotting them early and giving them the tools they need to build structure and resilience.

Self-initiated terrorists can escalate to action quickly, but a shallow ideology is easier to break *if* we act early, and the intervention provider is skilled. Once caught up in the radicalisation cycle, we are on the back foot; worse if they’re already

mobilising. Sharing sensitive information across agencies with differing levels of vetting adds to the complication, but there are solutions.

Such solutions include the proportionate lifetime management of offenders. In the UK, a Multi-Agency Centre—the MAC—was set up to reduce the likelihood of individuals re-engaging in terrorism, by sharing intelligence with a wider range of partners to deliver multiple interventions to better manage risk.

The partners' role is to collectively understand the risk posed by subjects referred by MI5 and CTP. The diversity of that partnership improves the range of interventions. Frontline partners are no longer distanced from the information they need to make effective decisions and provide better support through health, education, training, or critical thinking skills.

The MAC has solved the problem of moving sensitive nationally held information into local partners, lawfully. If that sounds easy, you have never written a data sharing agreement—and even if you have, I bet you haven't written one between a doctor and a spy!

But multi-agency interventions across the radicalisation and terrorist life-cycle are not learning from the past; it is anticipating future challenges. After 2017, we needed to make the management of terrorist suspects more explicit and consistent. Project Semper began as a result.

Semper will be a national service for the overt management of subjects to protect the public. The aim is sustained disengagement from extremism. UK policing is familiar with criminal offender management by mature multi-agency partnerships. CT nominal management is the same thing, except that not all our subjects have been convicted. It's about managing the risk either at the start of radicalisation or at any point up to and including their prison release after time served...and *potentially* forever. MAC and Semper are part of a set of extra-judicial sanctions, distinct from the PREVENT programme, which is voluntary and pre-crime.

Early intervention is becoming more challenging, with warnings less often seen in the real world but more commonly detected on line. To get ahead of the threat you have to see it coming—much harder today.

Online Harm

You can't contextualise or plan for future threats without understanding what's happening online. The scale and diversity of public forums has massively changed the game. All recent UK attacks have elements of online planning and radicalisation, sometimes very quickly. The Finsbury Park Mosque Extreme Right-Wing Terrorist went from a bitter, depressed thug to a radicalised murderer in just weeks.

The pandemic has increased online hateful extremism and radicalisation. Millions of people, many young, impressionable and lost, are cooped up for hours browsing online. It will increase the likelihood of keyboard extremists taking destructive fantasies into the real world, personally or through influence.

It's not my place to position the boundaries of free speech, but the *context* in which we consider free speech has undergone a seismic change in just a decade. The opportunities to speak or write anonymously are vast and dwarf the largest

real-world platforms of public discourse. There are great aspects to this, but we also understand the risks of anonymity; the behaviour it *can* drive in the vulnerable, and the effect of disinformation on society, selling lies, promoting paranoia and creating risk.

In 2021, few people challenge the view that online harms are a concern. How we make online safer is more controversial—it's a simple concept set within the most complex system, controlled by a powerful few.

Is a secure, safe Internet that also promotes freedoms of speech achievable? No one has the right to create and share criminal content online, but how do you define the boundary between lawful and unlawful discourse and who decides? How do we develop online law globally, when society's positions on freedom of expression differ even between culturally similar nations? How will a regulator enforce its will in this environment and how do providers satisfy everyone's demands. How do you negotiate with tech giants and innumerable smaller platforms? Where is the line between merely objectionable and dangerously extreme, and who decides? To tilt too far one way risks unacceptable state interference; too far the other way means the online Wild West.

For evidence, look no further than the 5G conspiracy theories. Cultivated in dark corners of Internet, they rapidly moved hundreds to take real world criminal action across international boundaries. Washington on 6 January 2021 probably wouldn't have happened without the amplification of social media.

This is where online meets reality and asks us to consider what 'incite' and 'radicalise' means in the information age. These concepts are difficult in law but we are stretching our understanding of proximity, causation and immediacy to extremes. Does incitement need to be directed or can it be passive? Can radicalisation be careless or reckless? Is asserting a 5G conspiracy an incitement to burn down masts, or simply an objectionable opinion? If we cannot prove the author's intent, do we work backwards from the consequences? And if so, how far do we stretch the chain of causation? Who is responsible? The espouser of the conspiracy? The Interviewer, the producer or the platform? Those who shared it?

Much of this responsibility sits with a powerful elite. Only big tech has the resources to fix this so I don't want a fight with them; after all, Alexander Graham-Bell invented the telephone, not heavy breathers. I have some sympathy for social media giants in control of tools unthinkably more powerful and influential than the original invention. But they now have an extraordinary responsibility to help us all solve a problem never previously contemplated.

But I will have no sympathy if they refuse to accept the burden or help solve it. The genie is out of the bottle and it shouldn't take someone like me to tell them it's dangerous. We don't want one of humanities' greatest inventions to become its greatest curse because we didn't co-operate to fix this social dilemma. I accept social media providers are not yet publishers in law—and therefore don't carry the same accountability for content—but they are receiving content at unfathomable scale, and *only they* are providing such an efficient mechanism for its wholesale distribution and a dangerous business model of echoes and amplification.

So only they can change how they manage it and how their users interact. *But* despite being in the best position to intervene, they are not best placed to decide

what to intervene in, *when* or *how*. The law needs to help them and then providers must proactively identify and prevent serious online criminal content and support law enforcement. They would also be wise to exercise social responsibility—strong terms and conditions of use that they rigorously enforce: and some have. But can they be consistent?

In the end, deciding what is and is not acceptable online has to be a decision for society as a whole. Perhaps, these ideas seem obvious, but even so, our approach must be cautious and the outcomes closely monitored. We have seen past problems with legislation and policy, intended as a scalpel, being applied like a sledgehammer that can lead to some Orwellian outcomes. This problem scales astronomically given the billions of social media users, and I do not underestimate the challenge the industry faces. But face it, it must.

The use of media to share harmful ideological messages is well understood. This tactic has been used to devastating effect by Daesh and we know what to look for. Other ideologies have learned from this example and can push hateful rhetoric just below the legal threshold as they fish for vulnerable minds to pull into hard-line extremism. They hide on encrypted platforms, luring in the vulnerable from more established networks.

But it's made more complex because hateful extremism as a concept is hard to pin down. We do not yet have a legal definition to enforce. Our challenge is the cliff edge between lawful *but* objectionable, and unlawful. The CT legal threshold creates a cliff edge where you can go from lawful to committing an offence with a 15-year prison sentence in a couple of key strokes. The absence of lower-level offences means that our intervention will almost always result in a very serious judicial outcome. Once you are in the serious end of the system, desistance and disengagement from extremism is far harder.

This is a criminal justice truism and the reason why we want to work to keep young people out of the system as much as possible. I'm proud of the incredible skill used to achieve a CT conviction. But there's also sadness. Many cases involve teenagers with issues that made them likely to be taken down this rabbit hole, like a recent case of a kid posting bomb-making manuals on Neo-Nazi forums. The 2-year suspended sentence reflected the seriousness of the case, and the mitigation required by his age and vulnerability. He should have been about to go to a top university not a top prison, and his parents were genuinely shocked. Youth, isolation and autism seem common factors in radicalisation susceptibility. Once a line is crossed, it's right we take action, but that should be tempered with rehabilitation, to reduce the risk of creating a harder terrorist long term.

The Prevent Pillar of the CONTEST Strategy

The environment, methods and terrorist types I describe has made the Protect & Pursue interventions *more* difficult—these tactics now feel like 'penalty kicks' that we cannot fail to save, but the chilling fact is that we have failed, and we will again.

So let's turn to the Prevent pillar—the *voluntary* support and de-radicalisation programme for people becoming extremists who have *not* been convicted of an offence. It's easily the most important pillar, given what I have described.

It's also there to prevent online harm and radicalisers being given a platform to preach. Both are controversial policies that tread the fine line of censorship in a democracy where free speech is a cornerstone but it is not an unqualified human right. There has to be the freedom to speak but not the freedom to do harm. But neither policy is as controversial it seems, as the one you would think would be far less so—the voluntary safeguarding of some of society's most vulnerable members.

Many people haven't even heard of Prevent, but we have allowed a loud, unchallenged minority to label it toxic—often for their own ends. And we made it easy for the critics, failing to be open and transparent or being clear on the difference between Prevent and Pursue—where our interventions were designed to protect and safeguard, and when they were designed to penalise and prosecute.

I have always wanted to talk more about the successes of Prevent than the effectiveness of Pursue. Prevent is about redemption, forgiveness and second chances. Prevent doesn't ruin lives—it saves them. It isn't just worthy—it's essential. If we didn't have it, we would need to invent it. Everything else I have said can be mitigated by early intervention and that starts in Prevent.

Research tells us that someone close to an extremist knows when the radicalisation cycle is gathering momentum. It's vital that the public can recognise this and report it, whilst trusting us to use that to help save lives. Our 'ACT Early' website is a resource we are proud of that is trying to generate that trust and confidence in the policy, explaining what we do and how we do it. It provides a simple public route into Prevent, with a clear call to action through a dedicated advice line staffed by specialists. It had an immediate operational impact with a genuine referral on day one, and many more since. Any single referral could be a life-saving intervention.

No matter how effective the other three pillars are, the only true cure is an effective Prevent system driven by communities looking out for their own. And there is no greater privilege than to Prevent the death of another human being.

As noted earlier, we must simultaneously look back for lessons and look forward for emerging threat. There are risks in getting this balance wrong. We must learn without getting stuck in 'fighting the last war'. Then again, it's no use scanning the horizon, when the enemy is at the gates.

Organisational learning is very different from individual learning, and it gets harder with scale. It's easy to get tunnel vision reviewing gaps in the system after an event. It can take resources away from engaging the most acute clear and present danger, looking for a single low risk, highly improbable event—a needle in an ever-bigger haystack.

We can't easily look at the tens of thousands of closed subjects in the hope of finding one that may return and ignore the 3000 we *know* are plotting against us. A deep understanding of terrorist behaviours as well as a sophisticated triage of intelligence fragments and tripwires to alert us are required. Machine learning against unfathomable quantities of data is essential. The scrutiny of something as complex as the CT Machine is a huge undertaking and can paralyse iterative

improvement—but recording lessons without implementing a change is like buying a book you never read.

Part of the answer is investing in a dedicated organisational development framework to make sure the lesson is captured, owned and docked into the right cross-system oversight and governance. This is easy to say but it mustn't become an un navigable bureaucracy, concerned only with large unwieldy projects. We have learned to our cost where vital learning was never operationalised, or was only applied to a very small part of the system. We must be experimental, agile, reflective and unafraid of failure, constantly testing our assumptions of best practice.

The biggest decisions, those on developing and deploying our data, science and technology, must be carefully made. Safeguards must be put in place to ensure such programmes don't live or die on personality or political expedience. Conversely, inertia cannot be a reason to continue with projects that are no longer relevant or failing. All these techniques must be underpinned by the highest ethics and public consent to avoid inadvertently becoming the very threat we are trying to counter. The ends do not justify the means if we want to maintain the virtues of a liberal democracy.

We should also invest in solutions that are threat-agnostic and can be re-purposed. This applies to tech, people, places and training. Given the pace of change and how quickly national security sometimes needs to pivot, being able to direct teams, systems, equipment and techniques to an entirely new problem, with minimal tweaks, is essential. Having the interoperability to bring in non-CT partners from major or organised crime is invaluable.

Afterword

One of the themes of this paper has been sharing, and better information sharing features in every inquiry. This is another thing that is easier to say than to do, as it requires regulation, expertise and management to share safely. And it requires real trust to do it *well*.

Now is the time to recognise that we must trust that our partners might know something we don't. Ironically, we can be blinded by our own expertise; the model we use to understand the world can determine what we see. Fresh minds and new perspectives; a diversity of thought is required if we are to be more than the sum of our parts and solve the most wicked problems I have shared with readers here.

And if we dare to share information, we must be constantly questioning what's working; exercise, test ourselves, learn what works well and then repeat. Exercise, test, learn and repeat. It bears repeating.

The Manchester Arena bombing will tell us we failed to learn what we already knew how to do; the Fishmongers Hall murder inquest has already told us we failed to anticipate an emerging threat. Those of us charged with defending the realm will have to live with those conclusions for the rest of our lives, and they weigh very heavily let me tell you.

But in my defence, I leave you with a few thoughts.

First, let me quote Anthony Hidden QC in the aptly named ‘Hidden Report’ into the 1988 Clapham Junction Rail Disaster, who said this:

There is almost no human action or decision that cannot be made to look flawed and less sensible in the misleading light of hindsight

And lastly, Matthew Syed, the wonderful author of *Bounce*, *Black Box Thinking*, and *Rebel Ideas*, who quoted Hidden in his Times column on 20 May 2021, went on to say:

These words should be pinned to the door of any future inquiry and used in response to anyone who rushes to judgment on front line professionals making decisions in complex circumstances. It is, I think, the only way to get to the truth. It is also the only way to subvert the false narratives that are threatening to harden into conventional wisdom.

I believe that CONTEST is a government strategy *entirely* fit for purpose—not something one can always say—and its 4 Ps are named pillars for a reason; take one away and the structure collapses. Without their counterparts, no single pillar will sustain the fight against terrorism, and we will never be able to rely too heavily on any single one.

Acknowledgements The author acknowledges the assistance of Detective Chief Inspector Will Lexton-Jones of SO15, who was his staff officer when he was Assistant Commissioner for Specialist Operations for 2 years and performed substantial work of fact finding, editing and many contributions to the early drafts of this paper; he was also an invaluable source of support for all public engagements discussing these matters. The author is also grateful for the work of his colleagues in the counter-terrorism roles he held during the relevant time periods:

Mar 2015–Sept 2016: Deputy Assistant Commissioner Specialist Operations MPS (DACSO) and Senior National Co-ordinator for Protect & Prepare

Oct 2016–Feb 2018: Deputy Assistant Commissioner and Senior National Co-ordinator for Pursue and Prevent

Mar 2018–July 2021: Assistant Commissioner Specialist Operations MPS (ACSO) and National Lead for CT Policing

Neil Basu is Assistant Commissioner of the Metropolitan Police Service, currently serving as Director of the Strategic Command Course, College of Policing, London, UK. From 2018 through 2021, he was the senior Counter-Terrorism leader for the UK. He was awarded the Queen’s Police Medal in 2016.

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.